REMARKS

In the Office Action mailed September 9, 2003, the Examiner noted that claims 1-10, 12-19 and 22-26 were pending, and rejected all claims. Claims 1, 7, 15-19 and 22-25 have been amended and, thus, in view of the forgoing claims 1-10, 12-19 and 22-26 remain pending for reconsideration which is requested. No new matter has been added. The Examiner's rejections are traversed below.

In the Office Action in the attached PTO-892 the Examiner lists Patent 5,748,736 as by "Issler et al". The inventor of Patent 5,748,736 is Mittra (see Patent 5,748,736 and page 4 of the Office Action). Correction of the PTO-892 is requested.

On page 2 of the Office Action the Examiner rejected claims 1, 3, 8, 9, 17, 22 and 23 under 35 U.S.C. § 102 as anticipated by Boebert. Page 4 of the Office Action rejects claims 6, 7, 10, 12 - 16 18 and 19 under 35 U.S.C. § 103 over Boebert and Mittra.

The Examiner particularly alleges that the Boebert enclave key is equivalent to the common key of the present invention ("An enclave key that corresponds to the recited common key ... ." - Action, page 2). The Boebert enclave key is a key protection type key as stated by Boebert:

> A personal keying device is assigned to each user in the enclave, and an enclave key is held in the protected storage in the server and in each of the workstations, and **used to protect other keys** stored or transmitted on the network.

(See Boebert col. 5, lines 48-51, **bold** emphasis supplied)

> Enclave Key
> There is one Enclave Key 40 per organization. It is held in protected storage in the Security Server 24 and the Crypto Media Controllers 26, and is **used to protect Media Keys 42** when they are being transmitted along the LAN 12.

(See Boebert col. 9, lines 63-67, **bold** emphasis supplied)

In cryptography the term "key" has a particular definition:

> key - In cryptography, the password needed to both encode and decipher a file. The key performs a sequence of operations on the original data. The recipient of the encoded file will need to apply another key in order to reverse all the operations in the correct order. Current encryption techniques such as Pretty Good Privacy (PGP) make use of a public key and a secret one.

(See Hutchinson Dictionary of Computers, Multimedia, and the Internet 2000)

In contrast, to a key that protects other keys as in Boebert, the keys (individual and common) of the present invention are designed to protect an electronic document type of electronic data (see application specification pages 1-3). The term "document" used in the specification and claims is consistent with the dictionary definition of same:

> document - Data associated with a particular application. For example, a text

> document might be produced by a word processor and a graphics document might be produced with a CAD package. An OMR or OCR document is a paper document containing data that can be directly input to the computer using a document reader.

(See Hutchinson Dictionary of Computers, Multimedia, and the Internet 2000)

As can be seen, a key is not an electronic document.

The equivalence or correspondence alleged by the Examiner is misplaced and withdrawal of the rejection as based on an inadequate foundation is requested.

In addition, in the present invention, an electronic document is data stored in a storage apparatus, to which a key management unit belongs, and is encrypted (for storage) using an individual key where the individual key is unique to said electronic data storage apparatus to which said management unit belongs. That is, when the document is stored a key for the apparatus is used. When this electronic document is transmitted to and received from other storage apparatuses, the document is encrypted or authenticated using a common key. These features are emphasized in independent claims 1, 15-17, 22 and 23. Claim 24 emphasizes the above-discussed features by characterizing the individual key as a local key that is "only" used for the local storage in which the key is stored and characterizing in the common key as a global key.

Boebert does not teach, disclose or suggest an individual (local) apparatus and common (global) keys as used with documents as in the present invention. In addition, Boebert does not teach or disclose an environment indicator indicating the environment of document transmission.

It is submitted that Boebert does not teach or suggest the invention of the independent claims.

With respect to dependent claim 6, the Examiner alleges that Mittra discloses the key management apparatus of the present invention equivalently as the GCS. This comparison is also misplaced. The GCS generates a group key for a multiple member group and a random key corresponding to each transmission, see:

> Once the GSC and the new member have authenticated each other and have agreed on a secret the GSC needs to provide the new member with information that will allow it to encrypt and/or decrypt the multicast transmission. At this point the GSC also needs to change the **group key (Kgrp)** which provides access to the multicast transmissions. This is done to prevent the joining member from decrypting previous transmissions to which it should not have access.
> Once the new Kgrp has been generated by the GSC, the current multicast group and the joining member all need to be apprised of the new Kgrp. To do this the GSC sends a multicast transmission containing the new Kgrp encrypted using the old Kgrp to the current multicast group telling them to now use the new Kgrp. This assumes that all senders are also receivers; if this is not the case, senders that

are not also receivers need to be notified individually using the separate secure channels the GSC maintains with each of the senders.

(Mittra, col. 8, lines 15-31, **bold** emphasis supplied)

3. Kencrypt=a random key chosen by the sender (or by the GSC which transmits it to the sender using the secure channel it has with the sender). **The random key must be changed after each message.** The generation of the random key is beyond the scope of this discussion (it may, for example, be generated using a pseudo-random number generator known in the art).

(Mittra, col. 10, lines 36-42, **bold** emphasis supplied)

As can be seen from the above discussion, no individual key and common key with the uses as in the present invention is taught or disclosed by Mittra

With respect to claim 7, Mittra, at col. 9, lines 54-61, notes that publicly available encryption algorithms can be used. This discussion says nothing about having an individual key for an apparatus, a common key for a group and a public key used for a different group of apparatuses as emphasized in claim 7.

As noted above, it is submitted that Mittra adds nothing to Boebert with respect to the features of the independent or dependent clams.

It is submitted that the invention of the claims distinguishes over the prior art and withdrawal of the rejection is requested.

It is submitted that the claims are not taught, disclosed or suggested by the prior art. The claims are therefore in a condition suitable for allowance. An early Notice of Allowance is requested.

If any further fees, other than and except for the issue fee, are necessary with respect to this paper, the U.S.P.T.O. is requested to obtain the same from deposit account number 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 1/8/3

By: /Randall Beckers/

J. Randall Beckers
Registration No. 30,358

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501